IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF NEW YORK

RAQUEL BRODY, *individually and on behalf of all others similarly situated*, Plaintiff, v. BERKSHIRE HATHAWAY, INC. and GOVERNMENT EMPLOYEES INSURANCE COMPANY, Defendants.	Case No. _____ **JURY TRIAL DEMANDED**

CLASS ACTION COMPLAINT

Plaintiff Raquel Brody (hereinafter, "Plaintiff"), individually and on behalf of all other persons similarly situated (the "Class" or "Class members"), by her undersigned attorneys, brings this Class Action Complaint against Berkshire Hathaway, Inc. ("Berkshire") and Government Employees Insurance Company ("GEICO") (collectively "Defendants"), and alleges the following based upon personal knowledge as to herself and her own actions, and, as to all other matters, allege, upon information and belief and investigation of her counsel.

NATURE OF THE ACTION

1. This class action arises out of the recent security breach of GEICO former and present customer's driver's license numbers ("Data Breach") at GEICO, one of the largest auto insurer in the United States. Due to Defendants' failure to safeguard confidential information, thousands of GEICO former and current customers have had their confidential information stolen.

2. As a result of the Data Breach, Plaintiff and Class Members suffered ascertainable losses in the form of loss of the value of their private and confidential information, out-of-pocket

expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the attack.

3. In addition, Plaintiff's, and Class Members' sensitive personal information—which was entrusted to GEICO—was compromised and unlawfully accessed due to the Ransomware Attack.

4. The Personally Identifiable Information ("PII") includes driver's license numbers. As a result of this Data Breach, false unemployment claims have been filed in the name of Plaintiff and Class Members.

5. On April 9, 2021 GEICO announced that between January 21, 2021 and March 1, 2021, hackers obtained unauthorized access to customers' driver's license numbers through GEICO's online sales system on their website and believe that this information could be used to fraudulently apply for unemployment benefits in the former and current customers' name.

6. Plaintiff brings this class action lawsuit on behalf of those similarly situated to address Defendants' inadequate safeguarding of Class Members' PII that it collected and maintained, and for failing to provide timely and adequate notice to Plaintiff and Class Members that their information had been subject to the unauthorized access and precisely what specific type of information was accessed.

7. Defendants maintained the PII in a reckless manner.

8. Upon information and belief, the potential for improper disclosure of Plaintiff's and Class Members' PII was a known risk to Defendants, and thus Defendants were on notice that failing to take steps necessary to secure the PII from those risks left that property in a dangerous condition.

9. In addition, Defendants and its employees failed to properly monitor the computer

network and systems that housed the PII. Had Defendants properly monitored its property, it would have discovered the Data Breach sooner.

10. Even though the threat of a data breach had been a well-known risk to Defendants, especially due to the valuable and sensitive nature of the data Defendants collect, store and maintain, Defendants failed to take reasonable steps to adequately protect the PII of its former and current customers.

11. The Data Breach was a direct result of Defendants' failure to implement adequate and reasonable cyber-security procedures and protocols necessary to protect PII.

12. As a result of Defendants' failure to take reasonable steps to adequately protect the ultra-sensitive PII of current and former Geico customers, Plaintiff's and Class members' PII is now in the hands of cyber-thieves whose motive and purpose was to illegally utilize that PII for profit.

13. The highly confidential PII that was compromised in the Data Breach is considered a valuable treasure trove that can be sold on the Dark Web and/or used to commit identity theft or other fraud for the foreseeable future.

14. Armed with the private information accessed in the Data Breach, data thieves can commit a variety of crimes including, e.g., filing for unemployment benefits and other governmental benefits, or aggregating it with other information to open new financial accounts in Class Members' names, take out loans in Class Members' names, file fraudulent tax returns using Class Members' information, obtain driver's licenses in Class Members' names but with another person's photograph, and give false information to police during an arrest.

15. As a result of the Data Breach, Plaintiff and Class Members have been exposed to a heightened and imminent risk of fraud and identity theft. Plaintiff and Class Members must now

and in the future closely monitor their financial accounts to guard against identity theft.

16. Plaintiff and Class Members may also incur out of pocket costs for, *e.g.*, purchasing credit monitoring services, credit freezes, credit reports, or other protective measures to deter and detect identity theft.

17. Defendants' failure to implement and follow proper security procedures has resulted in ongoing harm to Plaintiff and Class Members who will continue to experience a lack of data security for the indefinite future and remain at serious risk of identity theft and fraud that would result in significant monetary loss.

18. Plaintiff seeks to remedy these harms on behalf of herself and all similarly situated individuals whose PII was accessed during the Data Breach.

19. Plaintiff seeks to recover damages and other relief resulting from the Data Breach, including but not limited to, compensatory damages, reimbursement of out-of-pocket costs that Plaintiff and others similarly situated will be forced to bear, and declaratory judgment and injunctive relief, such as improvements to Defendants' data security system, future annual audits, and adequate credit monitoring services funded by Defendants; to mitigate future harms that are certain to occur in light of the scope of this breach.

20. Accordingly, Plaintiff brings this action against Defendants seeking redress for its unlawful conduct asserting claims for violation of the negligence and negligence *per se*, an intrusion upon seclusion, breach of an express and implied contract, breach of fiduciary duty, a breach of New York Business Law § 349.

PARTIES

A. Plaintiff Raquel Brody

21. Plaintiff Raquel Brody is a citizen and resident of the State of New York.

22. Plaintiff Brody is a former customer of GEICO but has not been a customer of

GEICO since 2017. Plaintiff Brody was notified by Defendants, via a Letter of Notice dated April 9. 2021, a copy of which is attached hereto as Exhibit A, that her PII, her driver's license number, was accessed without authorization and that as a result, the breached information might be used by thieves to apply for unemployment benefits. In fact, in the case of Plaintiff, this was not a mere theoretical scenario and in fact, as predicted, an attempt to illegally apply for unemployment benefits in Plaintiff's name following the Data Breach, was made. Plaintiff received a letter from the New York State Department of Labor stating that the Automated Clearing House network had rejected the direct deposit of her Unemployment Insurance benefit payments and would release her benefit payments to her debit card account instead. Plaintiff Brody had not applied for unemployment benefits.

B. Defendants

23. Defendant GEICO is an American auto insurance company with headquarters in Chevy Chase, Maryland. GEICO became a wholly owned subsidiary of Defendant Berkshire in 1996.

24. Defendant Berkshire has its headquarters located in Omaha, Nebraska.

JURISDICTION AND VENUE

25. This Court has subject matter jurisdiction pursuant to the Class Action Fairness Act of 2005, 28 U.S.C. § 1332(d)(2), because the aggregate amount in controversy exceeds $5 million, exclusive of interest and costs; and minimal diversity exists because at least one Plaintiff and the Defendants are citizens of different states.

26. This Court has personal jurisdiction over Defendants as GEICO conducts substantial business in this State and in this District and/or the conduct complained of occurred in and/or emanated from this State and District because Plaintiff's confidential information

compromised in Data Breach was likely stored and/or maintained in accordance with practices emanating from this District.

27. Venue is proper pursuant to 28 U.S.C. § 1391 because a substantial part of the events or omissions giving rise to the conduct alleged in this Complaint occurred in, were directed to, and/or emanated from this District.

FACTUAL ALLEGATIONS

Defendants' Business

28. GEICO is an American auto insurance company with headquarters in Chevy Chase, Maryland. It is the second largest auto insurer in the United States, after State Farm. GEICO is a wholly owned subsidiary of Berkshire Hathaway that provides coverage for more than 28 million motor vehicles owned by more than 17 million policy holders. GEICO writes private passenger automobile insurance in all 50 U.S. states and the District of Columbia. The insurance agency sells policies through local agents, called GEICO Field Representatives, over the phone directly to the consumer via licensed insurance agents, and through their website. GEICO is one of the fastest-growing major auto insurers in the United States that employs more than 40,000 associates and maintains 17 major offices around the country.[1]

29. GEICO's website has a Privacy Policy that states:

> Protecting your privacy is very important to us. Customers have trusted us with their insurance needs since 1936, and we take our obligation to safeguard and secure personal information very seriously. We want you to understand how we protect your privacy and when we collect, use, and share information.[2]

30. GEICO further assures customers that:

> We obtain information from you directly, from your transactions with us, and from third parties such as state motor vehicle departments.

[1] https://www.GEICO.com/about/corporate/at-a-glance/
[2] https://media.GEICO.com/legal/privacy_policy.htm

> We do not and will not sell your personal information.
> Any third parties who perform services for us are required to safeguard any personal information that they process on our behalf and may only use it to perform those services.
> We use technical and organizational measures to secure and limit access to your information.[3]

31. In addition, GEICO assures customers that their Private Information will be kept confidential and secure:

> We restrict access to your Information to employees who we have determined need it to provide products or services to you. We train our employees to safeguard customer information, and we require them to sign confidentiality and non-disclosure agreements. We maintain a variety of physical, electronic, and procedural safeguards to protect your Information from unauthorized access by third parties.[4]

The Data Breach

32. On or about April 9, 2021, GEICO announced that between January 21, 2021 and March 1, 2021, hackers used information to obtain unauthorized access to former and current customers' driver's license number through GEICO's online sales system on their website.

33. GEICO further warned former and current customers that fraudulent employment claims may have been the intended purposed of the breach and that they should be vigilant for any communications from state unemployment departments and agencies.

34. Upon discovering this incident, GEICO claims that they secured the data breach immediately and added "additional security enhancements" meant to curtail fraud.

35. GEICO did not disclose exactly how many former and present customers were impacted and failed to disclose the Data Breach until at least 6 weeks after it was discovered.

36. Tim Sadler, CEO of email security firm Tessian, points out why driver's license

[3] *Id.*
[4] *Id.*

numbers are very sought after by cyber criminals: " … It's a gold mine for hackers. With a driver's license number, bad actors can manufacture fake IDs, slotting in the number for any form that requires ID verification or use the information to craft curated social engineering phishing attacks."[5]

37. GEICO has stated that in this case, the hackers may be using these driver's license numbers to fraudulently apply for unemployment benefits in someone else's name. According to Sadler, this is a very lucrative scam for hackers and these license numbers are in "high demand."[6]

38. On information and belief, the PII data residing in GEICO's database(s) was not encrypted.

39. The cyberattack was reported to law enforcement.

40. Upon information and belief, the Data Breach was targeted at GEICO due to its status as one of the leading auto insurance providers in the United States.

41. Upon information and belief, the Data Breach was expressly designed to gain access to private and confidential data, including (among other things) the PII of the Plaintiff and the Class Members.

42. Defendants notified Plaintiff that her PII was stolen in the Data Breach. Plaintiff further believes that her stolen PII was subsequently sold on the Dark Web as is evidenced by the fact that an individual, not Plaintiff, fraudulently applied for fraudulent unemployment benefits in Plaintiff's name.

43. Upon informing GEICO's former and current customers that their PII was accessed without authorization, Defendants offered those impacted individuals a complimentary one-year

[5] https://www.cpomagazine.com/cyber-security/GEICO-data-breach-leaks-drivers-license-numbers-advises-customers-to-watch-out-for-fraudulent-unemployment-claims/
[6] Id.

subscription to the IdentityForce identity theft protection service.

44. The offer of credit and identity monitoring services is an acknowledgment by Defendants that the impacted customers are subject to an imminent threat of identity theft and financial fraud.

45. Despite acknowledging that data thieves accessed Plaintiff's and the Class Members' PII, Defendants did not begin to notify affected former and current customers until April 9, 2021.

46. Defendants had obligations created by contract, industry standards, common law, and representations made to Plaintiff and Class Members to keep their PII confidential and to protect it from unauthorized access and disclosure.

47. Plaintiff and Class Members provided their PII to Defendants with the reasonable expectation and mutual understanding that Defendants would comply with their obligations and representations to keep such information confidential and secure from unauthorized access.

48. Defendants failed to uphold its obligations to Plaintiff and Members of the Class. As a result, Plaintiff and Class Members have been significantly harmed and will be at a high risk of identity theft and financial fraud for many years to come.

The Data Breach was a Foreseeable Risk of which Defendants Were on Notice

49. The threat of hackers gaining access to information that businesses store is serious and well-known. Government authorities have been advising that companies take precautions to prevent these hacks for years.

50. Indeed, cyberattacks have become so notorious that the Federal Bureau of Investigation and U.S. Secret Service have issued warnings to potential targets so they are aware of, and prepared for, a potential attack.

51. Defendants' data security obligations were particularly important given the substantial increase in cyberattacks and/or data breaches preceding the date of the breach.

52. In light of recent high profile data breaches at other large companies, including, Microsoft (250 million records, December 2019), Wattpad (268 million records, June 2020), Facebook (267 million users, April 2020), Estee Lauder (440 million records, January 2020), Whisper (900 million records, March 2020), Advanced Info Service (8.3 billion records, May 2020), Defendants knew or should have known that its electronic records would be targeted by cybercriminals.[7]

53. Therefore, the recent increase in such attacks, and attendant risk of future attacks, was widely known to the public and the Defendants.

Defendants, At All Relevant Times, Had a Duty to Plaintiff and Class Members to Properly Secure their PII

54. Defendants, at all relevant times, had a duty to Plaintiff and Class Members to properly secure their PII, encrypt and maintain such information using industry standard methods, train its employees, utilize available technology to defend their systems from invasion, act reasonably to prevent foreseeable harm to Plaintiff and Class Members, and to promptly notify Plaintiff and Class Members when Defendants became aware of the potential that its current and former employees' PII, and their beneficiaries' and dependents PII, may have been compromised.

55. Defendants' duty to use reasonable security measures arose as a result of the special relationship that existed between Defendants, on the one hand, and Plaintiff and the Class Members, on the other hand. The special relationship arose because Plaintiff and the Members of the Class entrusted GEICO with their PII as part of receiving auto insurance coverage.

[7] See Maria Henriquez, The Top 10 Data Breaches of 2020, Security Magazine (Dec. 3, 2020), https://www.securitymagazine.com/articles/94076-the-top-10-data-breaches-of-2020 (last visited Dec. 18, 2020).

56. Defendants had the resources necessary to prevent the Data Breach but neglected to adequately invest in security measures, despite their obligation to protect such information. Accordingly, Defendants breached its common law, statutory, and other duties owed to Plaintiff and Class Members.

57. Defendants' duty to use reasonable security measures also arose under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data by entities like Defendants.

58. The Federal Trade Commission (FTC) has established data security principles and practices for businesses as set forth in its publication, Protecting Personal Information: A Guide for Business.

59. Among other things, the FTC states that companies should encrypt information stored on computer networks and dispose of consumer information that is no longer needed.[8]

60. The FTC also says to implement policies for installing vendor-approved patches to correct problems, and to identify operating systems.[9]

61. Additionally, the FTC also recommends that companies understand their network's vulnerabilities and develop and implement policies to rectify security deficiencies.[10]

62. Further, the FTC recommends that companies utilize an intrusion detection system to expose a data breach as soon as it occurs; monitor all incoming traffic for activity that might indicate unauthorized access into the system; monitor large amounts of data transmitted from the

[8] *See Protecting Personal Information*, Federal Trade Commission, https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited Dec. 18, 2020).
[9] *Id.*
[10] *Id.*

system; and have a response plan ready in the event of a data breach.[11]

63. In another FTC publication, Start with Security: A Guide for Business, the FTC recommends, among other things, that companies "make sure [third-party] service providers implement reasonable security measures."[12]

64. The FTC has prosecuted a number of enforcement actions against companies for failing to take measures to protect consumer data adequately and reasonably. The FTC has viewed and treated such security lapses as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45.

65. The Data Breach was a direct and proximate result of Defendants' failure to: (1) properly safeguard and protect Plaintiff's and Class Members' PII from unauthorized access, use, and disclosure, as required by various state and federal regulations, industry practices, and common law; (2) establish and implement appropriate safeguards to ensure the security and confidentiality of Plaintiff's and Class members' PII; and (3) protect against reasonably foreseeable threats to the security or integrity of such information.

66. Defendants failed to maintain reasonable data security procedures and practices.

67. Defendants also failed to implement reasonable security procedures and practices to prevent cyber attackers from unauthorized access to computer systems and network.

68. Defendants' failure to maintain and implement reasonable and appropriate measures to protect against unauthorized access to consumer PII constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

69. Accordingly, Defendants did not comply with legal state and federal law

[11] *Id.*
[12] *See Start With Security: A Guide for Business*, Federal Trade Commission, https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (last visited Dec. 18, 2020).

requirements, as discussed *supra*.

70. Defendants were at all times fully aware of their obligations to protect the PII of current and former customer. Defendants were also aware of the significant consequences that would result from their failure to do so.

Plaintiff and Class Members Have Been Injured and Will Suffer Additional Harm

71. To date, Defendants have merely offered complimentary identity theft and credit monitoring services for a period of one year. This offer, however, is wholly inadequate as it fails to provide for the fact that victims of data breaches and other unauthorized disclosures commonly face multiple years of ongoing identity theft and it entirely fails to provide any compensation for the unauthorized release and disclosure of Plaintiff's and Class Members' PII.

72. Furthermore, Defendants' identity theft and credit monitoring offer to Plaintiff and Class Members squarely places the burden on Plaintiff and Class Members, rather than on the Defendants, to investigate and protect themselves from Defendants' tortious acts resulting in the Data Breach. Rather than automatically enrolling Plaintiff and Class Members in identity theft and credit monitoring services upon discovery of the breach, Defendants merely sent instructions offering the services to affected employees, former employees, and their beneficiaries and dependents with the recommendation that they sign up for the services.

73. As a result of the Data Breach and Defendants' failure to provide timely notice to Plaintiff and Class Members, Plaintiff's, and Class Members' PII, including information associated with their beneficiaries and dependents, are now in the hands of unknown hackers. Plaintiff and Class Members now face an imminent heightened, and substantial risk of identity theft and other fraud, which is a concrete and particularized injury traceable to Defendants' conduct.

74. The consequences of Defendants' failure to keep Plaintiff's and Class members' PII and all information associated with their PII secure and protected are severe.

75. Thieves are already using the PII stolen to attempt to commit actual fraud and identity theft, as occurred to Plaintiff as alleged herein.

76. Theft of personal and financial information is a serious and growing problem in the United States.

77. Personal and financial information is a valuable commodity to identity thieves. As cyber security experts and journalists have recognized, the PII leaked in a data breach presents a treasure trove of information which could be sold on the Dark Web to other criminals and fraudsters to be used in countless illegal and fraudulent ways.

78. The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[13]

79. The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number."

80. The United States Government Accountability Office noted in a June 2007 report on Data Breaches ("GAO Report") that identify thieves use identifying data such as Social Security Numbers to open financial accounts, receive government benefits and incur charges and credit in

[13] *FTC Issues Final Rules on FACTA Identity Theft Definitions, Active Duty Alert Duration, and Appropriate Proof of Identity*, Federal Trade Commission (Oct. 24, 2004), https://www.ftc.gov/news-events/press-releases/2004/10/ftc-issues-final-rules-facta-identity-theft-definitions-active (last visited Dec. 18, 2020).

a person's name.[14] As the GAO Report states, this type of identity theft is the most harmful because it often takes some time for the victim to become aware of the theft, and the theft can impact the victim's credit rating adversely.[15]

81. Accordingly, identify theft victims must spend countless hours and large amounts of money repairing the impact to their credit.

82. PII is such a valuable commodity to identity thieves that once the information has been compromised, criminals often trade the information on the dark web for years. According to the GAO Report:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.

83. A 2014 study by the U.S. Department of Justice found that the average cost to a victim of identity theft is $1,343.[16]

84. According to a 2019 report, identity fraud caused nearly $17 billion in damage to victims and that the most common types of identity fraud are opening new credit card and bank accounts, business and personal loans, auto loans, and student loans.[17]

85. Indeed, data breaches and identity theft and financial fraud have a crippling effect on individuals and detrimentally impact the economy.

86. For all the above reasons, Plaintiff and Class Members have suffered harm; and

---

[14] U.S. Gov. Accountability Office, GAO-07-737, *Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Theft is Limited; However the Full Extent is Unknown* (2007).
[15] *Id.*
[16] *See* Cody Gredler, *The Real Cost of Identity Theft*, CSID (Sept. 9, 2016), https://www.csid.com/2016/09/real-cost-identity-theft/ (last visited Dec. 17, 2020).
[17] *See* Gayle Sato, *The Unexpected Costs of Identity Theft*, Experian (Sept. 30, 2020), https://www.experian.com/blogs/ask-experian/what-are-unexpected-costs-of-identity-theft/ (last visited Dec 17, 2020).

there is a substantial risk of injury to Plaintiff and Class Members that is imminent and concrete and that will continue for years to come.

87. As a direct and proximate result of Defendants' wrongful actions and inaction, Plaintiff and Class Members have suffered injury and damages, including the increased risk of identity theft, identity fraud, and financial fraud; improper disclosure of PII, the time and expense necessary to mitigate, remediate, and sort out the increased risk of identity theft and the inability to use debit cards because those cards were canceled, suspended, or otherwise rendered unusable as a result of the data breach, and/or false or fraudulent charges stemming from the data breaches.

CLASS ACTION ALLEGATIONS

88. Plaintiff brings this action and seeks to certify and maintain it as a class action under Federal Rules of Civil Procedure 23(a), (b)(2), (b)(3), and/or (c)(4), on behalf of herself, and the following proposed Classes (collectively, the "Class"):

> The **Nationwide Class** is defined as follows: All individuals residing in the United States whose PII was compromised in the Data Breach initially disclosed by GEICO in or about April 2021.
>
> The **New York Class** is defined as follows: All individuals residing in New York whose PII was compromised in the Data Breach initially disclosed by GEICO in or about April 2021.

89. Excluded from each of the above proposed Classes are: Defendants, any entity in which Defendants has a controlling interest, is a parent or subsidiary, or which is controlled by Defendants, as well as the officers, directors, affiliates, legal representatives, heirs, predecessors, successors, and assigns of Defendants; and judicial officers to whom this case is assigned and their immediate family members.

90. Plaintiff reserves the right to re-define the Class definitions after conducting discovery.

91. Each of the proposed Classes meets the criteria for certification under Rule 23(a), (b)(2), (b)(3) and/or (c)(4).

92. **Numerosity. Fed. R. Civ. P. 23(a)(1).** Pursuant to Rule 23(a)(1), the members of the Class are so numerous and geographically dispersed that the joinder of all members is impractical. While the exact number of Class Members is unknown to Plaintiff at this time, the proposed Class includes potentially tens of thousands of individuals whose Private Information was compromised in the Data Breach. Class members may be identified through objective means, including by and through Defendants' business records. Class Members may be notified of the pendency of this action by recognized, Court-approved notice dissemination methods, which may include U.S. mail, electronic mail, internet postings, and/or published notice.

93. **Commonality. Fed. R. Civ. P. 23(a)(2) and (b)(3).** Pursuant to Rule 23(a)(2) and with 23(b)(3)'s predominance requirement, this action involves common questions of law and fact that predominate over any questions affecting individual Class Members. The common questions include:

(a) Whether Defendants had a legal duty to implement and maintain reasonable security procedures and practices for the protection of Class Members' personal and financial information, including by vendors;

(b) Whether Defendants breached their legal duty to implement and maintain reasonable security procedures and practices for the protection of Plaintiff's and Class Members' personal and financial information;

(c) Whether Defendants' conduct, practices, actions, and omissions, resulted in or was the proximate cause of the Data Breach, resulting in the loss of personal and financial information of Plaintiff and Class Members;

(d) Whether Defendants had a legal duty to provide timely and accurate notice of the Data Breach to Plaintiff and Class Members;

(e) Whether Defendants breached their duty to provide timely and accurate notice of the Data Breach to Plaintiff and Class Members;

(f) Whether and when Defendants knew or should have known that GEICO's computer systems were vulnerable to attack;

(g) Whether Defendants failed to implement and maintain reasonable and adequate security measures, procedures, and practices to safeguard Plaintiff's and Class Members' personal and financial information, including by vendors;

(h) Whether Defendants breached implied contracts with Plaintiff and the Class in failing to have adequate data security measures despite promising to do so;

(i) Whether Defendants' conduct was negligent;

(j) Whether Defendants' conduct was *per se* negligent;

(k) Whether Defendants' practices, actions, and omissions constitute unfair or deceptive business practices;

(l) Whether Plaintiff and Class Members suffered legally cognizable damages as a result of Defendants' conduct, including increased risk of identity theft and loss of value of their personal and financial information; and

(m) Whether Plaintiff and Class members are entitled to relief, including damages and equitable relief.

94. **Typicality. Fed. R. Civ. P. 23(a)(3).** Pursuant to Rule 23(a)(3), Plaintiff's claims are typical of the claims of the members of the Class. Plaintiff, like all members of the Class, was injured through Defendants' uniform misconduct described above and asserts similar claims for relief. The same events and conduct that give rise to Plaintiff's claims also give rise to the claims of every other Class Member because Plaintiff and each Class Member is a person that has suffered harm as a direct result of the same conduct engaged in by Defendants and resulting in the Data Breach.

95. **Adequacy of Representation (Fed. R. Civ. P. 23(a)(4)**. Pursuant to Rule 23(a)(4), Plaintiff and her counsel will fairly and adequately represent the interests of the Class Members. Plaintiff has no interest antagonistic to, or in conflict with, the interests of the Class Members. Plaintiff's lawyers are highly experienced in the prosecution of consumer class actions and data breach cases.

96. **Superiority (Fed. R. Civ. P. 23(b)(3)**. Pursuant to Rule 23(b)(3), a class action is superior to individual adjudications of this controversy. Litigation is not economically feasible for individual members of the Class because the amount of monetary relief available to individual plaintiffs would be insufficient in the absence of the class action procedure. Separate litigation could yield inconsistent or contradictory judgments and increase the delay and expense to all parties and the court system. A class action presents fewer management difficulties and provides the benefits of a single adjudication, economy of scale, and comprehensive supervision by a single court.

97. **Risk of Inconsistent or Dispositive Adjudications and the Appropriateness of Final Injunctive or Declaratory Relief (Fed. R. Civ. P. 23(b)(1) and (2)).** In the alternative, this action may properly be maintained as a class action, because:

(a) the prosecution of separate actions by individual members of the Class would create a risk of inconsistent or varying adjudication with respect to individual members of the Class, which would establish incompatible standards of conduct for Defendants; or

(b) the prosecution of separate actions by individual members of the Class would create a risk of adjudications with respect to individual members of the Class which would, as a practical matter, be dispositive of the interests of other members of the Class not parties to the adjudications, or substantially impair or impede their ability to protect their interests; or

(c) Defendants have acted or refused to act on grounds generally applicable to the Class, thereby making appropriate final injunctive or corresponding declaratory relief with respect to the Class as a whole.

98. **Issue Certification (Fed. R. Civ. P. 23(c)(4)**. In the alternative, the common questions of fact and law, set forth in Paragraph 93, are appropriate for issue certification on behalf of the proposed Class.

COUNT I

NEGLIGENCE
(On Behalf of Plaintiff and all Classes)

99. Plaintiff re-alleges and incorporates by reference all paragraphs as if fully set forth herein.

100. Defendants required Plaintiff and GEICO current and former customers who are Class Members to submit non-public, sensitive personal and financial information for purposes of receiving auto insurance with Defendants.

101. Defendants had (and continue to have) a duty to Plaintiff and Class Members to

exercise reasonable care in safeguarding and protecting their personal and financial information. Defendants also had (and continue to have) a duty to use ordinary care in activities from which harm might be reasonably anticipated (such as in the storage and protection of personal and financial information within their possession, custody and control and that of their vendors).

102. Defendants' duty to use reasonable security measures arose as a result of the special relationship that existed between Defendants and their employees. Only Defendants were able to ensure that the data retention and computer systems were sufficient to protect against the harm to Plaintiff and the Class Members from a data breach.

103. Pursuant to the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45, Defendants had a duty to provide fair and adequate computer systems and data security to safeguard the personal and financial information of Plaintiff and Class Members.

104. The FTCA prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendants, of failing to use reasonable measures to protect the personal and financial information of Plaintiff and Class Members. The FTC publications and orders described above also form part of the basis of Defendants' duty in this regard.

105. Defendants required, gathered, and stored personal and financial information of Plaintiff and Class Members for purposes of providing them with auto insurance policies.

106. Defendants violated the FTCA by failing to use reasonable measures to protect the personal and financial information of Plaintiff and Class Members and not complying with applicable industry standards, as described herein.

107. Plaintiff and Class Members are within the class of persons that the FTC Act was intended to protect.

108. The harm that occurred as a result of the Data Breach is the type of harm the FTCA was intended to guard against. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and Class Members.

109. Defendants violated these standards and duties by failing to exercise reasonable care in safeguarding and protecting Plaintiff's and Class Members' PII by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems to safeguard and protect the personal and financial information entrusted to it – including Plaintiff' and Class Members' PII. It was reasonably foreseeable to Defendants that its failure to exercise reasonable care in safeguarding and protecting Plaintiff's and Class Members' PII, by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems, would result in the unauthorized release, disclosure, and dissemination of Plaintiff's and Class Members' PII.

110. Defendants, by and through their negligent actions, inaction, omissions, and want of ordinary care, unlawfully breached their duties to Plaintiff and Class Members by, among other things, failing to exercise reasonable care in safeguarding and protecting Plaintiff' and Class Members' PII within their possession, custody and control.

111. Defendants, by and through their negligent actions, inactions, omissions, and want of ordinary care, further breached their duties to Plaintiff and Class Members by failing to design, adopt, implement, control, direct, oversee, manage, monitor and audit its processes, controls, policies, procedures, protocols, and software and hardware systems for complying with the

applicable laws and safeguarding and protecting their PII.

112. But for Defendants' negligent breach of the above-described duties owed to Plaintiff and Class Members, their PII would not have been released, disclosed, and disseminated without their authorization.

113. Plaintiff's and Class Members' PII was transferred, sold, opened, viewed, mined and otherwise released, disclosed, and disseminated to unauthorized persons without their authorization as the direct and proximate result of Defendants' failure to design, adopt, implement, control, direct, oversee, manage, monitor and audit their processes, controls, policies, procedures and protocols for complying with the applicable laws and safeguarding and protecting Plaintiff's and Class Members' PII.

114. Defendants' above-described wrongful actions, inaction, omissions, and want of ordinary care that directly and proximately caused this Data Breach constitute negligence.

115. As a direct and proximate result of Defendants' above-described wrongful actions, inaction, omissions, and want of ordinary care that directly and proximately caused the Data Breach, Plaintiff and Class Members have suffered (and will continue to suffer) ongoing, imminent, and impending threat of identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; loss of the confidentiality of the stolen confidential data; the illegal sale of the compromised data on the dark web; expenses and/or time spent on credit monitoring and identity theft insurance; time spent scrutinizing bank statements, credit card statements, and credit reports; expenses and/or time spent initiating fraud alerts, decreased credit scores and ratings; lost work time; and other economic and non-economic harm. At minimum and alternatively, Plaintiff alleges and asserts that the acts and omissions of Defendants have caused to Plaintiff and the Class

nominal damages.

COUNT II

BREACH OF IMPLIED CONTRACT
(On Behalf of Plaintiff and the Classes)

116. Plaintiff re-alleges and incorporates by reference all paragraphs as if fully set forth herein.

117. Defendants required Plaintiff and current and former customers of GEICO to provide their PII, including names, addresses, driver's license numbers and other personal information, as a condition of obtaining an auto insurance policy.

118. As a condition of Plaintiff's and Class Members' obtaining auto insurance policies with Defendants, they provided their PII to Defendants. In so doing, Plaintiff and Class Members entered into implied contracts with Defendants by which Defendants agreed to safeguard and protect such information, to keep such information secure and confidential, and to timely and accurately notify Plaintiff and Class Members if their data had been breached and compromised, or stolen.

119. Plaintiff and Class Members fully performed their obligations under the implied contracts with Defendants.

120. Defendants breached the implied contracts it made with Plaintiff and Class Members by failing to safeguard and protect their PII, and by failing to provide timely and accurate notice to them that personal and financial information, along with the personal information of their beneficiaries and dependents, was compromised as a result of the Data Breach.

121. As a direct and proximate result of Defendants' above-described breach of implied contract, Plaintiff and Class Members have suffered (and will continue to suffer) ongoing, imminent, and impending threat of identity theft crimes, fraud, and abuse, resulting in monetary

loss and economic harm; actual identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; loss of the confidentiality of the stolen confidential data; the illegal sale of the compromised data on the dark web; expenses and/or time spent on credit monitoring and identity theft insurance; time spent scrutinizing bank statements, credit card statements, and credit reports; expenses and/or time spent initiating fraud alerts, decreased credit scores and ratings; lost work time; and other economic and non-economic harm.

COUNT III

VIOLATIONS OF THE DRIVER'S PRIVACY PROTECTION ACT 18 U.S.C. §§ 2721, *et seq.* ("DPPA") (On Behalf of Plaintiff and the Classes)

122. Plaintiff re-alleges and incorporates all previous allegations as though fully set forth herein.

123. The DPPA, 18 U.S.C. § 2722(a), prohibits any person, organization, or entity from knowingly obtaining or disclosing "personal information, from a motor vehicle record, for a purpose not permitted under [§ 2721(b) of the DPPA]."

124. The DPPA defines "motor vehicle record" to mean "any record that pertains to a motor vehicle operator's permit, motor vehicle title, motor vehicle registration, or identification card issued by a department of motor vehicles." 18 U.S.C. § 2725(1).

125. The DPPA defines "personal information" to mean "information that identifies an individual, including an individual's photograph, social security number, driver identification number, name, address (but not the 5-digit zip code), telephone number, and medical or disability information, but does not include information on vehicular accidents, driving violations, and driver's status." 18 U.S.C. § 2725(3).

126. Defendant GEICO is a contractor and/or vendor with the New York State

Department of Motor Vehicles including, *inter alia*, partnering with the NYS DMV to allow use of electronic identification cards on their smart phones and other electronic devices.

127. In violation of the DPPA, Defendants knowingly disclosed the PII, including the driver's license identification numbers, of Plaintiff and other Class Members by storing that information on its systems without adequate protection.

128. Consistent with the way they were programmed and configured by Defendants' unsecured systems disclosed Plaintiff's and Class Members' PII to unauthorized individuals.

129. Pursuant to 18 U.S.C. § 2724(b), as a result of Defendants' violation of the DPPA, Plaintiff's and Class Members are entitled to actual damages, but not less than liquidated damages in the amount of $2,500.

COUNT IV

VIOLATION OF THE NEW YORK GENERAL BUSINESS LAW § 349
(On Behalf of Plaintiff and the Nationwide Class, Or, Alternatively, Plaintiff Brody and the New York Class)

130. Plaintiff re-alleges and incorporates by reference all paragraphs as if fully set forth herein.

131. Defendants engaged in deceptive, unfair, and unlawful trade acts or practices in the conduct of trade or commerce and furnishing of services, in violation of N.Y. Gen. Bus. Law § 349(a), including but not limited to the following:

(a) Defendants misrepresented material facts to Plaintiff and the Class by representing that they would maintain adequate data privacy and security practices and procedures to safeguard Class Members' PII from unauthorized disclosure, release, data breaches, and theft;

(b) Defendants misrepresented material facts to Plaintiff and the Class by representing that they did and would comply with the requirements of

federal and state laws pertaining to the privacy and security of Class Members' PII;

(c) Defendants omitted, suppressed, and concealed material facts of the inadequacy of its privacy and security protections for Class Members' PII;

(d) Defendants engaged in deceptive, unfair, and unlawful trade acts or practices by failing to maintain the privacy and security of Class Members' PII, in violation of duties imposed by and public policies reflected in applicable federal and state laws, resulting in the Data Breach. These unfair acts and practices violated duties imposed by laws including the Federal Trade Commission Act (15 U.S.C. § 45);

(e) Defendants engaged in deceptive, unfair, and unlawful trade acts or practices by failing to disclose the Data Breach to the Class in a timely and accurate manner, contrary to the duties imposed by N.Y. Gen. Bus. Law § 899-aa(2).

132. Defendants knew or should have known that the GEICO computer systems and data retention and security practices and systems were inadequate to safeguard the Class Members' PII entrusted to it, and that risk of a data breach or theft was highly likely.

133. Defendants should have disclosed this information because Defendants were in a superior position to know the true facts related to the defective data security.

134. Defendants' failure constitutes false and misleading representations, which have the capacity, tendency, and effect of deceiving or misleading consumers (including Plaintiff and Class Members) regarding the security of GEICO's network and aggregation and retention of PII.

135. The representations upon which consumers (including Plaintiff and Class

Members) relied were material representations (e.g., as to Defendants' adequate protection of PII), and consumers (including Plaintiff and Class Members) relied on those representations to their detriment.

136. Defendants' conduct is unconscionable, deceptive, and unfair, as it is likely to, and did, mislead consumers acting reasonably under the circumstances. As a direct and proximate result of Defendants' conduct, Plaintiff and other Class Members have been harmed, in that they were not timely notified of the Data Breach, which resulted in profound vulnerability to their personal information and other financial accounts.

137. As a direct and proximate result of Defendants' unconscionable, unfair, and deceptive acts and omissions, Plaintiff's and Class Members' PII was disclosed to third parties without authorization, causing and will continue to cause Plaintiff and Class Members damages.

138. Defendants' acts, conducts and omissions complained of or related to, were consumer-oriented acts, conducts and omissions.

139. Plaintiff and Class Members seek relief under N.Y. Gen. Bus. Law § 349(h), including, but not limited to, actual damages, treble damages, statutory damages, injunctive relief, and/or attorney's fees and costs.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of the members of the Classes defined above, respectfully request that this Court:

A. Certify this case as a class action under Federal Rule of Civil Procedure 23, appoint Plaintiff as the Class representatives, and appoint the undersigned as class counsel;

B. Order appropriate relief to Plaintiff and the Classes;

C. Enter injunctive and declaratory relief as appropriate under the applicable law;

D. Award Plaintiff and the Classes pre-judgment and/or post-judgment interest as

prescribed by law;

E. Award reasonable attorneys' fees and costs as permitted by law; and

F. Enter such other and further relief as may be just and proper.

DEMAND FOR JURY TRIAL

Plaintiff hereby demand a trial by jury of all claims so triable.

DATED: May 4, 2021

By: _____
Gary S. Graifman
Melissa R. Emert
KANTROWITZ, GOLDHAMER & GRAIFMAN, P.C.
747 Chestnut Ridge Road
Chestnut Ridge, New York 10977
Telephone: (845) 356-2570
Facsimile: (845) 356-4335
ggraifman@kgglaw.com
memert@kgglaw.com

Attorneys for Plaintiff and the Proposed Class